PCT/EP 00/07122

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

8/2

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

EP 00/07122

4

Aktenzeichen:	199 35 945.8
Anmeldetag:	30. Juli 1999
Anmelder/Inhaber:	Giesecke & Devrient GmbH, München/DE
Bezeichnung:	Verfahren, Datenträger sowie System zur Authentisierung eines Benutzers und eines Endgeräts
IPC:	G 07 C, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 03. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weihmayr

A 9161
06/00
EDV-L

Verfahren, Datenträger sowie System zur Authentisierung eines Benutzers und eines Endgeräts

Die vorliegende Erfindung betrifft allgemein die Authentisierung bei der Benutzung von Datenträgern wie Chipkarten und dergleichen, und insbesondere ein Authentisierungsverfahren, einen Datenträger sowie ein Authentisierungssystem umfassend einen Datenträger und ein Endgerät (Terminal).

Zum Nachweis, daß ein Benutzer zur Benutzung einer Chip- oder Magnetstreifenkarte tatsächlich berechtigt bzw. autorisiert ist, dient üblicherweise eine individuelle Geheimzahl, beispielsweise eine sogenannte PIN (Persönliche Identifizierungs Nummer). Die PIN ist auf der Karte gespeichert und wird, nachdem die Karte in ein Endgerät eingeführt worden ist, mit der dem Endgerät von dem Benutzer angegebenen PIN verglichen. Ist der Vergleich positiv, so kann vom Endgerät z. B. auf geschützte Bereiche der Chipkarte, beispielsweise Speicherbereiche, zugegriffen werden.

Die Benutzung von PINs ist problematisch, weil die Karte in Kenntnis der PIN von jedermann benutzt werden kann. Die Karte ist also nicht an den eigentlichen Karteninhaber, sondern an den PIN-Inhaber gebunden. Durch freiwillige oder unfreiwillige Weitergabe der PIN ist somit ein Mißbrauch der Karte möglich. PINs sind auch insofern unsicher, als sie einerseits vergessen und andererseits ausgespäht werden können.

Selbst wenn sich ein berechtigter Benutzer durch Eingabe seiner PIN ausgewiesen hat, ist das System nur teilweise autorisiert - nämlich der Benutzer gegenüber der Karte beziehungsweise dem Endgerät. Eine Autorisierung des Endgeräts gegenüber der Karte oder dem Benutzer findet nicht statt. Handelt es sich um ein gefälschtes Endgerät, so besteht die Gefahr, daß die PIN mittels dem gefälschten Endgerät ausgespäht wird. Die PIN allein stellt

daher keine ausreichende Sicherung dar, weil eine Authentisierung des Endgeräts gegenüber der Karte bzw. gegenüber dem Benutzer fehlt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, den Authentisierungsvorgang sicherer zu gestalten. Insbesondere besteht die der Erfindung zugrunde liegende Aufgabe darin, ein Authentisierungsverfahren, ein Authentisierungssystem bestehend aus Datenträger und Endgerät und einen Datenträger zur Authentisierung sowohl des Benutzers als auch des Terminals vorzuschlagen, wodurch die individuelle Berechtigung des Benutzers und die Echtheit des Terminals überprüfbar sind.

Diese Aufgabe wird erfindungsgemäß durch ein Authentisierungsverfahren, einen Datenträger und ein Authentisierungssystem gemäß den nebengeordneten Ansprüchen gelöst.

In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung angegeben.

Der erfindungsgemäßen Lösung liegt der Gedanke zugrunde, daß der Authentisierungsvorgang sicherer gestaltet werden kann, wenn zunächst die Echtheit des Terminals geprüft wird und dem Terminal anschließend biometrische Daten des Benutzers präsentiert werden. Biometrische Daten, wie ein Fingerabdruck oder dergleichen, sind im Gegensatz zu einer PIN eindeutig benutzerspezifisch. Durch das vorherige Prüfen der Echtheit des Terminals wird gewährleistet, daß ein Ausspähen der sensiblen, benutzerspezifischen biometrischen Daten verhindert wird. Das Prüfen der Echtheit des Endgeräts geschieht in der Weise, daß ein auf dem Datenträger fest gespeicherter Geheimcode, der nur dem Benutzer bekannt ist, von dem Endgerät ausgelesen und dem Benutzer angezeigt wird. Nur wenn der Geheimcode korrekt ange-

zeigt wird, wird der Benutzer dem Endgerät das biometrische Merkmal präsentieren, um sich gegenüber dem Endgerät bzw. dem Datenträger als berechtigter Benutzer auszuweisen. Der Geheimcode kann auf dem Datenträger auf einem nur durch autorisierte Endgeräte zugreifbaren Speicherplatz gespeichert sein und/oder nur von einem autorisierten Endgerät korrekt entschlüsselt werden.

Nachdem die Authentisierung des Terminals erfolgt ist, wird durch Präsentieren des benutzerspezifischen biometrischen Merkmals und Vergleich der von dem biometrischen Merkmal erfaßten Daten mit auf dem Datenträger gespeicherten biometrischen Daten, im Gegensatz zum PIN-Vergleich, eine benutzerindividuelle Authentisierung gegenüber dem Datenträger bzw. dem Endgerät erreicht.

Zusätzlich zur biometrischen Authentisierung des Benutzers kann eine PIN-Authentisierung des Benutzers durch Eingabe einer PIN und Vergleich der eingegebenen PIN mit auf dem Datenträger gespeicherter PIN erfolgen.

Die Erfindung wird nachfolgend beispielhaft anhand der einzigen Figur dargestellt.

Der in der Figur dargestellte Authentisierungsvorgang umfaßt drei Schritte, von denen der zweite Schritt auch entfallen kann.

Im ersten Schritt liest ein Endgerät T (Terminal) von einem ersten Speicherbereich eines Datenträgers C, beispielsweise einer Chipkarte, einen Geheimcode (CODE) aus und präsentiert diesen CODE dem Benutzer U (User). Der CODE ist auf der Chipkarte C beispielsweise auf einem zugriffsgeschützten Speicherplatz und/oder in verschlüsselter Form abgespeichert, so daß der

CODE nur von einem "echten" Terminal T, das entweder zugriffsberechtigt ist oder den Entschlüsselungsalgorithmus kennt, ausgelesen und dem Benutzer U angezeigt werden kann.

Wenn der Benutzer U den von dem Terminal T ausgelesenen CODE als seinen Geheimcode wiedererkennt, wird er die weiteren Authentisierungsschritte vornehmen. Im dargestellten Fall wird er dem Terminal T zunächst seine PIN angeben. Die PIN wird dann, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet, wo sie entschlüsselt und mit einer auf der Chipkarte C abgespeicherten PIN verglichen wird, und dem Terminal T wird anschließend das Ergebnis des Vergleichs mitgeteilt. Der Datentransfer, insbesondere der Transfer des CODE's, der PIN und der nachfolgend noch zu beschreibenden biometrischen Daten BIO erfolgt vorzugsweise in verschlüsselter Form, um ein Ausspähen dieser sensiblen Daten zu erschweren.

Sofern der PIN-Vergleich positiv war ("OK"), führt das Terminal T den Authentisierungsprozeß fort, indem nunmehr die benutzerindividuelle Authentisierung mittels biometrischer Merkmale des Benutzers erfolgt. Dazu präsentiert der Benutzer dem Terminal T ein biometrisches Merkmal, beispielsweise einen Fingerabdruck oder die Iris eines Auges. Das biometrische Merkmal wird vom Terminal T erfaßt und in biometrische Daten BIO umgewandelt, die, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet werden. Dort werden die eingelesenen biometrischen Daten des Benutzers mit auf der Chipkarte C gespeicherten biometrischen Daten verglichen. Im Falle eines positiven Vergleichs ("OK") wird das Terminal T für die Eingabe weiterer Benutzerkommandos freigegeben.

Patentansprüche

1. Verfahren zum Authentisieren eines Benutzers (U) eines Datenträgers (C) zur berechtigten Benutzung des Datenträgers und zum Authentisieren eines Datenträgerendgerätes (T) zum berechtigten Zugreifen des Datenträgerendgerätes auf Speicherbereiche des Datenträgers, umfassend folgenden Schritte:

- Auslesen eines Geheimcodes (CODE) von dem Datenträger (C) durch das Datenträgerendgerät (T),
- Präsentieren des ausgelesenen Geheimcodes (CODE) gegenüber dem Benutzer (U),
- Präsentieren eines biometrischen Merkmals (BIO) eines Benutzers (U),
- Vergleichen des präsentierten biometrischen Merkmals (BIO) mit einem auf dem Datenträger (C) gespeicherten biometrischen Merkmal.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß dem Terminal (T) desweiteren eine PIN präsentiert wird, die mit einer auf dem Datenträger (C) gespeicherten PIN verglichen wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß als biometrisches Merkmal (BIO) ein Fingerabdruck eines Benutzers (U) verwendet wird.

4. Datenträger (C) zur Authentisierung eines Endgeräts gegenüber einem Benutzer und des Benutzers gegenüber dem Datenträger, umfassend einen ersten Speicherbereich, in dem ein Geheimcode (CODE) derart abgespeichert ist, daß der Geheimcode von einem Datenträgerendgerät (T) auslesbar und anzeigbar ist, und einen zweiten Speicherbereich, in dem biometrische Daten abgespeichert sind.

5. Datenträger nach Anspruch 4, **dadurch gekennzeichnet,** daß in einem dritten Speicherbereich eine PIN abgespeichert ist.

6. Datenträger nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet,** daß durch biometrischen Daten durch einen Fingerabdruck generiert werden.

7. Authentisierungssystem umfassend einen Datenträger (C) mit Speicherbereichen und ein Datenträgerendgerät (T) zum Zugreifen auf die Speicherbereiche des Datenträgers, **dadurch gekennzeichnet,** daß

- der Datenträger (C) einen ersten Speicherbereich für die Speicherung eines Geheimcodes (CODE) und einen zweiten Speicherbereich für die Speicherung biometrischer Daten,
- das Datenträgerendgerät (T) eine erste Einrichtung zum Auslesen des Geheimcodes (CODE) aus dem ersten Speicherbereich und Präsentieren des ausgelesenen Geheimcodes auf einem Display, sowie eine zweite Einrichtung zum Einlesen biometrischer Daten (BIO), und
- eine Einrichtung zum Vergleichen der eingelesenen biometrischen Daten (BIO) mit im zweiten Speicherbereich gespeicherten biometrischen Daten im Datenträger (C) und/oder im Datenendgerät (T).

aufweist.

8. Authentisierungssystem nach Anspruch 7, **dadurch gekennzeichnet,** daß der Datenträger (C) einen dritten Speicherbereich für die Speicherung einer PIN aufweist.

9. Authentisierungssystem nach Anspruch 7 oder 8, **dadurch gekennzeichnet,** daß die gespeicherten biometrischen Daten durch einen Fingerabdruck generiert werden.

Zusammenfassung

Im Zusammenhang mit der Benutzung von Datenträgern wie Chipkarten C und dergleichen wird vorgeschlagen, daß sich zunächst das Endgerät T, in dem die Chipkarte C verarbeitet wird, gegenüber dem Benutzer U authentisiert und sich anschließend der Benutzer U gegenüber dem Datenträger C bzw. dem Endgerät T authentisiert. Die Authentisierung des Endgeräts gegenüber dem Benutzer U erfolgt durch Auslesen eines CODE's von dem Datenträger C und Präsentieren des ausgelesenen CODE's gegenüber dem Benutzer U, der diesen CODE als richtig oder falsch präsentiert einstuft. Wenn das Endgerät T einen richtigen CODE präsentiert hat, authentisiert sich der Benutzer U gegenüber der Chipkarte C bzw. dem Endgerät T indem er ein biometrisches Merkmal BIO präsentiert, beispielsweise seinen Fingerabdruck. Durch diese Verfahrensweise wird sichergestellt, daß das biometrische Merkmal BIO des Benutzers U nicht von einem gefälschten Endgerät T ausgespäht werden kann.

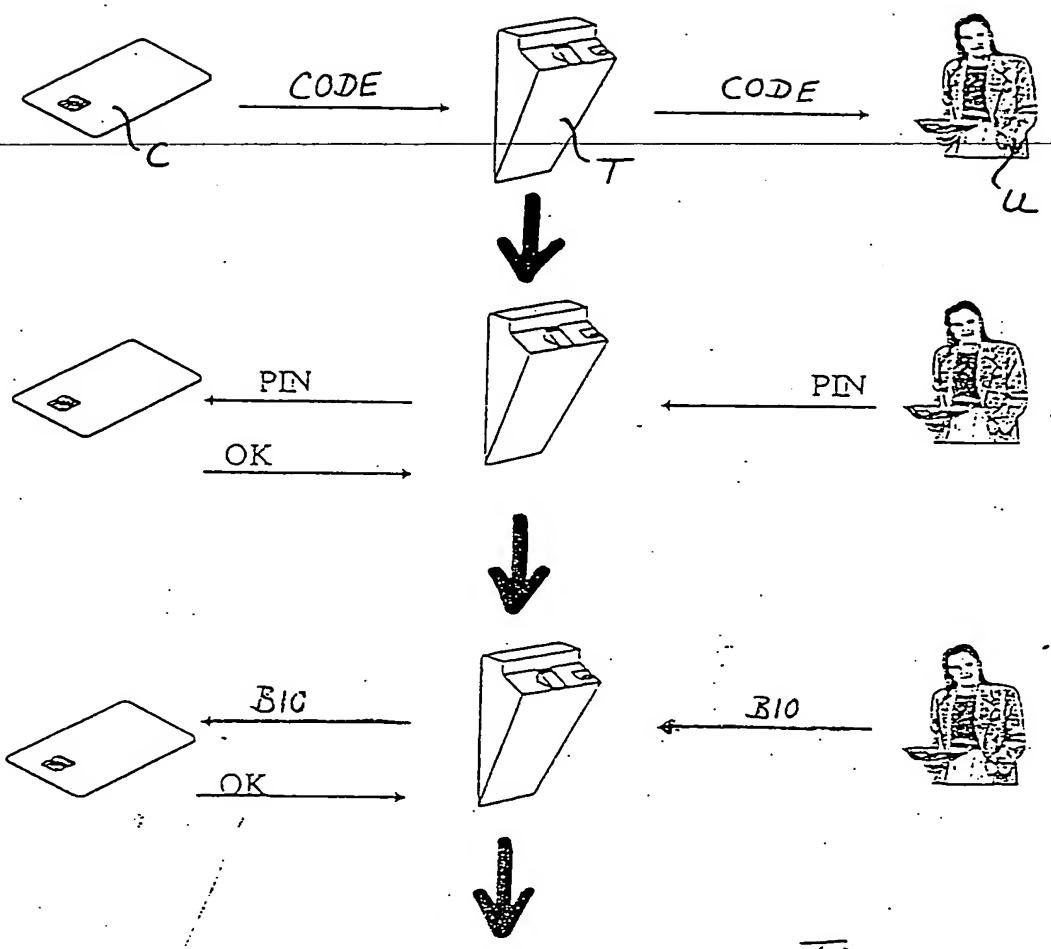

Fig.